Abstract

Method and apparatus for modular multiplying and calculating unit for modular multiplying

In a method for modular multiplying a multiplicand by a multiplier using a modulus, the multiplicand, the multiplier and the modulus being polynomials of variable, a multiplication look-ahead method to obtain a multiplication shift value is carried out. An intermediate result polynomial is shifted to the left by the number of digits of the multiplication shift value to obtain a shifted intermediate result polynomial. Furthermore, a reduction look-ahead method to obtain a reduction shift value is carried out, the reduction shift value equalling the difference of the degree of the shifted intermediate result polynomial and the degree of the modulus polynomial. The modulus polynomial is then shifted by a number of digits equalling the reduction shift value to obtain a shifted modulus polynomial. In a three-operands addition, the shifted intermediate result polynomial and the multiplicand are summed and the shifted modulus polynomial is subtracted to obtain an updated intermediate result polynomial. By iteratively executing the preceding steps the modular multiplication is processed progressively until all the powers of the multiplier polynomial have been processed. By means of a carry disabling function it is possible to carry out both a **Z**/N**Z** arithmetic as well as a GFarithmetic on a single long number calculating unit.

Fig. 2